

What is claimed is:

1           1.       A method of transmitting a signal, comprising:  
2           generating a sequence of pseudorandom noise chips at a base power level;  
3           increasing the power level of a first group of the sequence of chips above the base  
4 power level; and  
5           increasing the power level of a second group of the sequence of chips above the base  
6 power level, wherein an interval of the first and second groups of the sequence of chips are  
7 related according to a varying relationship.

1           2.       The method of claim 1, wherein the varying relationship is an interval  
2 separating the first and second groups of the sequence of chips determined according to a  
3 cryptographic algorithm.

1           3.       The method of claim 1, wherein the power level of the first group of the chip  
2 sequence is different than the power level of the second group of the chip sequence.

1           4.       The method of claim 1, wherein the power levels of the first and second  
2 groups of the chip sequence are substantially greater than the base power level.

1           5.       A method of receiving a signal including a code having boosted and non-  
2 boosted portions, wherein the boosted portions are separated by the non-boosted portions  
3 according to a predetermined algorithm, the method comprising:  
4           generating a local version of the code; partial sequences of a predetermined code,  
5 wherein the partial sequences are related by a predetermined algorithm separating the partial  
6 sequences by variable length intervals;  
7           correlating the code with the received signal;  
8           generating a decoding signal according to the predetermined algorithm;  
9           detecting, based on the correlation and the decoding signal, boosted portions of the  
10 received signal having one or more power levels higher than a power level of non-boosted  
11 portions of the received signal; and  
12           determining a phase of the predetermined code based on the detected boosted portions  
13 of the received signal.

1           6.       The method of claim 5, wherein the predetermined algorithm is a  
2 cryptographic algorithm.

1           7.       The method of claim 6, wherein the cryptographic algorithm varies an interval  
2 of non-boosted portions of the signal in an encrypted manner.

1           8.       The method of claim 5, wherein said one or more power levels of the boosted  
2 portions of the received signal is substantially greater than the power level of the non-boosted  
3 portions of the received signal.

1           9        A computer signal embodied in a carrier wave, comprising:  
2 a plurality of groups of low power chips;  
3 a plurality of groups of high power chips, wherein the groups of low power chips are  
4 disposed between the groups of the high power chips and lengths of the groups of low power  
5 chips vary, and wherein the high power chips upon reception are suitable for processing by a  
6 computer.

1           10.      The computer signal according to claim 9, wherein the lengths of the groups of  
2 low power chips vary according to a predetermined cryptographic algorithm.

1           11.      The computer signal according to claim 9, wherein the lengths of the groups of  
2 high power chips are fixed.

1           12.      The computer signal according to claim 9, wherein a power level of the high  
2 power chips is substantially greater than a power level of the low power chips.

1           13.      A transmitter suitable for transmitting a staggered pulse signal, comprising:  
2 a code generator configured to generate a plurality of pulses according to a code;  
3 a cryptographical unit configured to generate a cryptographical sequence based on a  
4 cryptographical key; and  
5 an amplifier connected to the code generator and the cryptographical unit and  
6 configured to amplify a first one of the pulses to a first level and to amplify a second one of  
7 the pulses to a second level in response to the cryptographical sequence.

1           14.      The transmitter of claim 13, wherein the code is a pseudorandom noise (PN)  
2 code.

1 15. The transmitter of claim 13, wherein the amplifier is configured to respond to  
2 the cryptographical sequence to generate an interval between the first and second pulses that  
3 is determined based on the cryptographical sequence.

1 16. A transmitter suitable for transmitting a staggered pulse signal, comprising:  
2 code generator means for generating a plurality of pulses according to a code;  
3 means for generating a cryptographical sequence based on a cryptographical key; and  
4 amplifier means for amplifying a first one of the pulses of the code to a first level and  
5 amplifying a second one of pulses of the code to a second level based on the cryptographical  
6 sequence.

1 17. The transmitter of claim 16, wherein the code is a pseudorandom noise (PN)  
2 code.

1 18. The transmitter of claim 16, wherein the amplifier means responds to the  
2 cryptographical sequence to generate an interval between the first and second pulses that is  
3 determined based on the cryptographical sequence.

1 19. A receiver for receiving a staggered pulse signal having high-power pulses of  
2 a code separated by intervals according to a cryptographic algorithm, the receiver  
3 comprising:

4 a cryptographic unit configured to generate a cryptographic sequence corresponding  
5 to the cryptographic algorithm;

6 a code detection unit connected to the cryptographic unit and configured to detect a  
7 code phase of the received staggered pulse signal based on the cryptographic sequence  
8 generated by the cryptographic unit.

1 20. The receiver of claim 19, wherein the code detection unit comprises:  
2 a correlator configured to correlate the received signal with a local code and to output  
3 a correlation signal; and

4 a decoder unit configured to decode the correlated signal based on the cryptographic  
5 sequence generated by the cryptographic unit.

1 21. The receiver of claim 20, wherein the decoder unit comprises a matched filter  
2 configured to detect a sequence of intervals between the high power pulses of the received  
3 signal corresponding to the cryptographic sequence.

1           22.     The receiver of claim 21, wherein the cryptographic unit comprises a  
2 cryptographic processing unit and a cryptographic storage unit having stored therein  
3 cryptographic keys, wherein the cryptographic processing unit generates the cryptographic  
4 sequence based on a key stored in the cryptographic storage unit.

1           23.     The receiver of claim 19, wherein the code of the staggered pulse signal is a  
2 pseudorandom noise (PN) code.

1           24.     A receiver for receiving a staggered pulse signal having high-power pulses of  
2 a code separated by intervals according to a cryptographic algorithm, the receiver  
3 comprising:  
4           means for generating a cryptographic sequence corresponding to the cryptographic  
5 algorithm;  
6           code detection means for detecting a code phase of the received staggered pulse signal  
7 based on the generated cryptographic sequence.

1           25.     The receiver of claim 24, wherein said code detection means comprises:  
2           means for correlating the received signal with a local code and outputting a  
3 correlation signal; and  
4           decoder means for decoding the correlated signal based on the generated  
5 cryptographic sequence.

1           26.     The receiver of claim 25, wherein said decoder means comprises filter means  
2 for detecting a sequence of intervals between the high power pulses of the received signal  
3 corresponding to the cryptographic sequence.

1           27.     The receiver of claim 24, wherein the code of the staggered pulse signal is a  
2 pseudorandom noise (PN) code.